

# The IT Governance Institute™ is pleased to offer you this complimentary download of COBIT®

COBIT provides good practices for the management of IT processes in a manageable and logical structure, meeting the multiple needs of enterprise management by bridging the gaps between business risks, technical issues, control needs and performance measurement requirements. If you believe as we do, that COBIT enables the development of clear policy and good practices for IT control throughout your organisation, we invite you to support ongoing COBIT research and development.

There are two ways in which you may express your support: (1) Purchase COBIT through the Association (ISACA) Bookstore (please see the following pages for order form and Association membership application. Association members are able to purchase COBIT at a significant discount); (2) Make a generous donation to the Information Systems Audit and Control Foundation, which sponsors the IT Governance Institute.

The complete COBIT package consists of all six publications, an ASCII text diskette, four COBIT implementation/orientation Microsoft® PowerPoint® presentations and a CD-ROM. A brief overview of each component is provided below. Thank you for your interest and support of COBIT!

For additional information about the IT Governance Institute visit [www.ITgovernance.org](http://www.ITgovernance.org)

## ***Management Guidelines***

To ensure a successful enterprise, you must effectively manage the union between business processes and information systems. The new *Management Guidelines* is composed of Maturity Models, Critical Success Factors, Key Goal Indicators and Key Performance Indicators. These *Management Guidelines* will help answer the questions of immediate concern to all those who have a stake in enterprise success.

## ***Executive Summary***

Sound business decisions are based on timely, relevant and concise information. Specifically designed for time-pressed senior executives and managers, the COBIT *Executive Summary* consists of an Executive Overview which explains COBIT's key concepts and principles.

## ***Framework***

A successful organization is built on a solid framework of data and information. The *Framework* explains how IT processes deliver the information that the business needs to achieve its objectives. This delivery is controlled through 34 high-level control objectives, one for each IT process, contained in the four domains. The *Framework* identifies which of the seven information criteria (effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability), as well as which IT resources (people, applications, technology, facilities and data) are important for the IT processes to fully support the business objective.

## ***Audit Guidelines***

Analyze, assess, interpret, react, implement. To achieve your desired goals and objectives you must constantly and consistently audit your procedures. *Audit Guidelines* outlines and suggests actual activities to be performed corresponding to each of the 34 high-level IT control objectives, while substantiating the risk of control objectives not being met.

## ***Control Objectives***

The key to maintaining profitability in a technologically changing environment is how well you maintain control. COBIT's *Control Objectives* provides the critical insight needed to delineate a clear policy and good practice for IT controls. Included are the statements of desired results or purposes to be achieved by implementing the 318 specific, detailed control objectives throughout the 34 high-level control objectives.

## ***Implementation Tool Set***

An Implementation Tool Set, which contains Management Awareness and IT Control Diagnostics, Implementation Guide, frequently asked questions, case studies from organizations currently using COBIT and slide presentations that can be used to introduce COBIT into organizations. The tool set is designed to facilitate the implementation of COBIT, relate lessons learned from organizations that quickly and successfully applied COBIT in their work environments and assist management in choosing implementation options.

## ***CD-ROM***

The CD-ROM, which contains all of COBIT, is published as a Folio infobase. The material is accessed using Folio Views®, which is a high-performance, information retrieval software tool. Access to COBIT's text and graphics is now easier than ever, with flexible keyword searching and built-in index links (optional purchase).

*A network version (multi-user) of COBIT 3rd Edition will be available. It will be compatible with Microsoft Windows NT/2000 and Novell NetWare environments. Contact the ISACA Bookstore for pricing and availability.*

**See Order Form, Donation Information and Membership Application on the following pages.**

# ISACF Contribution Form

Contributor: \_\_\_\_\_

Address: \_\_\_\_\_  
\_\_\_\_\_

City \_\_\_\_\_ State/Province \_\_\_\_\_

Zip/Postal Code \_\_\_\_\_ Country \_\_\_\_\_

Remitted by: \_\_\_\_\_

Phone: \_\_\_\_\_

e-mail: \_\_\_\_\_

For information on the Foundation and  
contribution benefits see [www.isaca.org/finfo.htm](http://www.isaca.org/finfo.htm)

## Contribution amount (US \$):

☐ \$25 (donor) ☐ \$100 (Silver) ☐ \$250 (Gold)

☐ \$500 (Platinum) ☐ Other US \$ \_\_\_\_\_

☐ Check enclosed payable in US \$ to ISACF

☐ Charge my: ☐ VISA

☐ MasterCard

☐ American Express

☐ Diners Club

Card number \_\_\_\_\_ Exp. Date \_\_\_\_\_

Name of cardholder: \_\_\_\_\_

Signature of cardholder: \_\_\_\_\_

Complete card billing address if different from address on left  
\_\_\_\_\_  
\_\_\_\_\_

U.S. Tax ID number: 95-3080691

Fax your credit card contribution to ISACF at +1.847.253.1443, or mail your contribution to:  
ISACF, 135 S. LaSalle Street, Department 1055, Chicago, IL 60674-1055 USA

**Direct any questions to Scott Artman at +1.847.253.1545, ext. 459 or [finance@isaca.org](mailto:finance@isaca.org)**

**Thank you for supporting COBIT!**

## Recent ISACF Research Projects



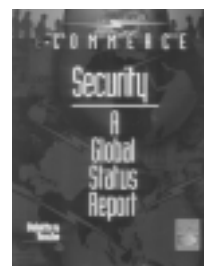
**Control Objectives for  
Net Centric Technology, NCC**  
Member - \$90 Non-member - \$130



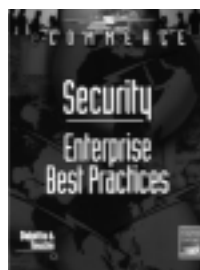
**Digital Signatures  
Security & Controls, ISDS**  
Member - \$35 Non-member - \$50

In Partnership with

**Deloitte &  
Touche**



**e-Commerce Security**  
A Global Status Report, ISEC  
Member - \$35 Non-member - \$50



**e-Commerce Security**  
Enterprise Best Practices, 2-EC  
Member - \$30 Non-member - \$40



**e-Commerce Security**  
Trading Partner Identification,  
Registration and Enrollment, TRS-1  
Member - \$35 Non-member - \$50

For additional information on these publications and others offered through the Bookstore, please visit [www.isaca.org/pubs1.htm](http://www.isaca.org/pubs1.htm)

# Pricing and Order Form



	CODE	ISACA Members	Non-Members
Complete COBIT® 3rd Edition®	CB3S CB3SC	\$70 (text only) \$115 (text and CD-ROM)	\$225 (text and CD-ROM)

COBIT 2nd Edition purchasers - see [www.isaca.org/3upgrade.htm](http://www.isaca.org/3upgrade.htm) for special upgrade pricing.  
Individual components are also available for purchase:

	CODE	ISACA Members	Non-Members
Executive Summary	CB3E	\$3	\$3
Management Guidelines	CB3M	\$40	\$50
Framework	CB3F	\$15	\$20
Control Objectives	CB3C	\$25	\$30
Audit Guidelines	CB3A	\$50	\$155
Implementation Tool Set	CB3I	\$15	\$20

All prices are US dollars. Shipping is additional to all prices.

Name \_\_\_\_\_ Date \_\_\_\_\_

ISACA Member: ☐ Yes ☐ No Member Number \_\_\_\_\_

If an ISACA Member, is this a change of address? ☐ Yes ☐ No

Company Name \_\_\_\_\_

Address: ☐ Home ☐ Company \_\_\_\_\_

City \_\_\_\_\_ State/Province \_\_\_\_\_ Country \_\_\_\_\_ Zip/Mail Code \_\_\_\_\_

Phone Number ( ) \_\_\_\_\_ Fax Number ( ) \_\_\_\_\_

E-mail Address \_\_\_\_\_ Special Shipping Instructions or Remarks \_\_\_\_\_

Code	Title/Item	Quantity	Unit Price	Total
<i>All purchases are final. All prices are subject to change.</i>				<b>Subtotal</b>
Illinois (USA) residents, add 8.25% sales tax, or Texas (USA) residents, add 6.25% sales tax Shipping and Handling – see chart below				
				<b>TOTAL</b>

## PAYMENT INFORMATION – PREPAYMENT REQUIRED

☐ Payment enclosed. Check payable in U.S. dollars, drawn on U.S. bank, payable to the Information Systems Audit and Control Association.

☐ Charge to ☐ VISA ☐ MasterCard ☐ American Express ☐ Diners Club

(Note: All payments by credit card will be processed in U.S. Dollars)

Account # \_\_\_\_\_ Exp. Date \_\_\_\_\_

Print Cardholder Name \_\_\_\_\_ Signature of Cardholder \_\_\_\_\_

Cardholder Billing Address if different than above \_\_\_\_\_

## Shipping and Handling Rates

For orders totaling	Outside USA and Canada	Within USA and Canada
Up to US\$30	\$7	\$4
US\$30.01 - US\$50	\$12	\$6
US\$50.01 - US\$80	\$17	\$8
US\$80.01 - US\$150	\$22	\$10
Over US\$150	15% of total	10% of total

Please send me information on: ☐ Association membership ☐ Certification ☐ Conferences ☐ Seminars ☐ Research Projects

## ISACA BOOKSTORE

135 SOUTH LASALLE, DEPARTMENT 1055, CHICAGO, IL 60674-1055 USA

TELEPHONE: +1.847.253.1545, EXT. 401 FAX: +1.847.253.1443 E-MAIL: [bookstore@isaca.org](mailto:bookstore@isaca.org)

WEB SITE: [www.isaca.org/pubs1.htm](http://www.isaca.org/pubs1.htm)



## MEMBERSHIP APPLICATION

☐ MR. ☐ MS. ☐ MRS. ☐ MISS ☐ OTHER \_\_\_\_\_

Date \_\_\_\_\_  
MONTH/DAY/YEAR

Name \_\_\_\_\_  
FIRST MIDDLE LAST/FAMILY

PRINT NAME AS YOU WANT IT TO APPEAR ON MEMBERSHIP CERTIFICATE

Residence address \_\_\_\_\_  
STREET  
CITY STATE/PROVINCE/COUNTRY POSTAL CODE/ZIP

Residence phone \_\_\_\_\_ AREA/COUNTRY CODE AND NUMBER  
Residence facsimile \_\_\_\_\_ AREA/COUNTRY CODE AND NUMBER

Company name \_\_\_\_\_

Business address \_\_\_\_\_  
STREET  
CITY STATE/PROVINCE/COUNTRY POSTAL CODE/ZIP

Business phone \_\_\_\_\_ AREA/COUNTRY CODE AND NUMBER  
Business facsimile \_\_\_\_\_ AREA/COUNTRY CODE AND NUMBER

E-mail \_\_\_\_\_

**Send mail to**

- ☐ Home  
☐ Business

**Form of Membership requested**

- ☐ Chapter Number (see reverse)  
☐ Member at large (no chapter within 50 miles/80 km)  
☐ Student (must be verified as full-time)  
☐ Retired (no longer seeking employment)

- ☐ I do not want to be included on a mailing list, other than that for Association mailings.

**How did you hear about ISACA?**

- 1 ☐ Friend/Co-worker 6 ☐ Local Chapter  
2 ☐ Employer 7 ☐ CISA Program  
3 ☐ Internet Search 8 ☐ Direct Mail  
4 ☐ IS Control Journal 9 ☐ Educational Event  
5 ☐ Other Publication

**Current field of employment (check one)**

- 1 ☐ Financial  
2 ☐ Banking  
3 ☐ Insurance  
4 ☐ Transportation  
5 ☐ Retail & Wholesale  
6 ☐ Government/National  
7 ☐ Government/State/Local  
8 ☐ Consulting  
9 ☐ Education/Student  
10 ☐ Education/Instructor  
11 ☐ Public Accounting  
12 ☐ Manufacturing  
13 ☐ Mining/Construction/Petroleum  
14 ☐ Utilities  
15 ☐ Other Service Industry  
16 ☐ Law  
17 ☐ Health Care  
99 ☐ Other

**Level of education achieved**

(indicate degree achieved, or number of years of university education if degree not obtained)

- 1 ☐ One year or less 7 ☐ AS  
2 ☐ Two years 8 ☐ BS/BA  
3 ☐ Three years 9 ☐ MS/MBA/Masters  
4 ☐ Four years 10 ☐ Ph.D.  
5 ☐ Five years 99 ☐ Other  
6 ☐ Six years or more

**Certifications obtained (other than CISA)**

- 1 ☐ CPA 7 ☐ FCA  
2 ☐ CA 8 ☐ CFE  
3 ☐ CIA 9 ☐ MA  
4 ☐ CBA 10 ☐ FCPA  
5 ☐ CCP 11 ☐ CFSA  
6 ☐ CSP 12 ☐ CISSP  
99 ☐ Other

**Work experience**

(check the number of years of Information Systems work experience)

- 1 ☐ No experience 4 ☐ 8-9 years  
2 ☐ 1-3 years 5 ☐ 10-13 years  
3 ☐ 4-7 years 6 ☐ 14 years or more

**Current professional activity (check one)**

- 1 ☐ CEO  
2 ☐ CFO  
3 ☐ CIO/IS Director  
4 ☐ Audit Director/General Auditor  
5 ☐ IS Security Director  
6 ☐ IS Audit Manager  
7 ☐ IS Security Manager  
8 ☐ IS Manager  
9 ☐ IS Auditor  
10 ☐ External Audit Partner/Manager  
11 ☐ External Auditor  
12 ☐ Internal Auditor  
13 ☐ IS Security Staff  
14 ☐ IS Consultant  
15 ☐ IS Vendor/Supplier  
16 ☐ IS Educator/Student  
99 ☐ Other

Date of Birth \_\_\_\_\_  
MONTH/DAY/YEAR

**Payment due**

- Association dues \$ 110.00 (US)  
• OR student/retired dues (\$55 US) \$ \_\_\_\_\_ (US)  
• Chapter dues (see the following page) \$ \_\_\_\_\_ (US)  
• New Member processing fee \$ 30.00 (US)\*  
PLEASE PAY THIS TOTAL \$ \_\_\_\_\_ (US)

\* Membership dues consist of Association dues, Chapter dues and New Member processing fee. (Processing fee does not apply to Student/Retired Members.)

**Method of payment**

- ☐ Check payable in U.S. dollars, drawn on U.S. bank  
☐ Send invoice\*\*  
☐ MasterCard ☐ VISA ☐ American Express ☐ Diners Club

All payments by credit card will be processed in US\$'s

\*\* Applications cannot be processed until dues payment is received.

ACCT # \_\_\_\_\_

Print Name of Cardholder \_\_\_\_\_

Expiration Date \_\_\_\_\_  
MONTH/DAY/YEAR

Signature \_\_\_\_\_

Cardholder billing address if different than address provided above: \_\_\_\_\_

By accepting membership to the Information Systems Audit and Control Association, members agree to hold the Association and the Information Systems Audit and Control Foundation, its officers, directors, agents, trustees, and employees, harmless for all acts or failures to act while carrying out the purpose of the Association and the Foundation as set forth in its respective bylaws.

Initial payment entitles New Members to membership beginning the first day of the month following the date payment is received by International Headquarters through the end of that year. No rebate of dues is available upon early resignation of membership.

Contributions or gifts to the Information Systems Control Association are not tax-deductible as charitable contributions in the United States. However, they may be tax-deductible as ordinary and necessary business expenses.

Membership dues allocated to a 1-year subscription to the *IS Control Journal* are as follows: \$45 for U.S. Members, \$60 for non-U.S. members. This amount is non-deductible from dues.

**Make checks payable to:**

Information Systems Audit and Control Association

**Mail your application and check to:**

Information Systems Audit and Control Association  
135 S. LaSalle, Dept. 1055  
Chicago, IL 60674-1055 USA  
Phone: +1.847.253.1545 x470 or x405  
Fax: +1.847.253.1443

**Contact the chapter in your area or the International Office for information on chapter dues if the amount is not listed below. Additional chapter information may be found at [www.isaca.org/chap1.htm](http://www.isaca.org/chap1.htm)**

Chapter Name	Chapter Number	Dues	Chapter Name	Chapter Number	Dues	Chapter Name	Chapter Number	Dues	Chapter Name	Chapter Number	Dues
<b>ASIA</b>			Netherlands	97	\$30	New York Metropolitan	10	\$50	Willamette Valley, OR (Portland)	50	\$30
Hong Kong	64	\$35	Lagos, Nigeria	149	\$20	Western New York (Buffalo)	46	\$30	Utah (Salt Lake City)	04	\$30
Bangalore, India	138	\$15	Oslo, Norway	74	\$40	Harrisburg, PA	45	\$30	Mt. Rainier, WA (Olympia)	129	\$20
Calcutta	165	*	Warsaw, Poland	151	\$0	Lehigh Valley (Allentown, PA)	122	\$35	Puget Sound, WA (Seattle)	35	\$35
Coimbatore, India	155	*	Slovenia	137	\$50	Philadelphia, PA	06	\$40	<b>OCEANIA</b>		
Delhi, India	140	\$10	Slovensko	160	\$40	Pittsburgh, PA	13	\$20	Adelaide, Australia	68	\$0
Hyderabad, India	164	\$17	South Africa	130	\$50	National Capital Area, DC	05	\$30	Brisbane, Australia	44	\$16
Madras, India (Chennai)	99	\$5	Madrid, Spain	112	*	<b>Southeastern United States</b>			Canberra, Australia	92	\$30
Mumbai, India	145	\$20	Sweden	88	\$45	North Alabama (Birmingham)	65	\$30	Melbourne, Australia	47	\$30
Pune, India	159	\$17	Switzerland	116	\$35	Jacksonville, FL	58	\$30	Perth, Australia	63	\$5
Indonesia	123	*	London, UK	60	\$88	Central Florida (Orlando)	67	\$30	Sydney, Australia	17	\$30
Nagoya, Japan	118	*	Central UK	132	\$35	South Florida (Miami)	33	\$40	Auckland, New Zealand	84	\$24
Osaka, Japan	103	*	Northern UK	111	\$50	West Florida (Tampa)	41	\$35	Wellington, New Zealand	73	\$22
Tokyo, Japan	89	\$180	<b>NORTH AMERICA</b>			Atlanta, GA	39	\$30	Papua New Guinea	152	\$0
Korea	107	\$30	<b>Canada</b>			Charlotte, NC	51	\$35	<b>To receive your copy of the Information Systems Control Journal, please complete the following subscriber information:</b>		
Malaysia	93	\$10	Calgary, AB	121	\$0	Research Triangle (Raleigh, NC)	59	\$25	<b>Size of Organization (at your primary place of business):</b>		
Muscat, Oman	167	*	Edmonton, AB	131	\$25	Piedmont/Triad (Winston-Salem, NC)	128	\$30	① <input type="checkbox"/> Fewer than 50 employees		
Karachi, Pakistan	148	\$12.50	Vancouver, BC	25	\$15	Greenville, SC	54	\$30	② <input type="checkbox"/> 50-100 employees		
Manila, Philippines	136	\$25	Victoria, BC	100	\$0	Memphis, TN	48	\$45	③ <input type="checkbox"/> 101-500 employees		
Jeddah, Saudi Arabia	163	\$0	Winnipeg, MB	72	\$15	Middle Tennessee (Nashville)	102	\$45	④ <input type="checkbox"/> More than 500 employees		
Riyadh, Saudi Arabia	154	\$0	Nova Scotia	105	\$0	Virginia (Richmond)	22	\$30	<b>What is the size of your professional audit staff? (local office)</b>		
Singapore	70	\$10	Ottawa Valley, ON	32	\$10	<b>Southwestern United States</b>			① <input type="checkbox"/> 1 individual		
Sri Lanka	141	\$15	Toronto, ON	21	\$25	Central Arkansas (Little Rock)	82	\$60	② <input type="checkbox"/> 2-5 individuals		
Taiwan	142	\$35	Montreal, PQ	36	\$15	Central Mississippi (Jackson)	161	\$25	③ <input type="checkbox"/> 6-10 individuals		
Bangkok, Thailand	109	\$9	Quebec City, PQ	91	\$35	Denver, CO	16	\$35	④ <input type="checkbox"/> 11-25 individuals		
UAE	150	\$10	<b>Islands</b>			Greater Kansas City, KS	87	\$25	⑤ <input type="checkbox"/> More than 25 individuals		
<b>CENTRAL/SOUTH AMERICA</b>			Bermuda	147	\$0	Baton Rouge, LA	85	\$25	<b>Your level of purchasing authority:</b>		
Buenos Aires, Argentina	124	\$150	Trinidad & Tobago	106	\$25	Greater New Orleans, LA	61	\$20	① <input type="checkbox"/> Recommend Products/Services		
Mendoza, Argentina	144	\$120	<b>Midwestern United States</b>			St. Louis, MO	11	\$25	② <input type="checkbox"/> Approve Purchase		
São Paulo, Brazil	166	\$25	Chicago, IL	02	\$50	New Mexico (Albuquerque)	83	\$25	③ <input type="checkbox"/> Recommend and Approve Purchase		
Santiago de Chile	135	\$40	Illini (Springfield, IL)	77	\$30	Central Oklahoma (OK City)	49	\$30	<b>Education courses attended annually (check one)</b>		
Bogota, Colombia	126	\$50	Central Indiana (Indianapolis)	56	\$25	Tulsa, OK	34	\$25	① <input type="checkbox"/> None		
San Jose, Costa Rica	31	\$33	Michiana (South Bend, IN)	127	\$25	Austin, TX	20	\$25	② <input type="checkbox"/> 1		
Merida, Yucatan, Mexico	101	\$50	Iowa (Des Moines)	110	\$25	Greater Houston Area, TX	09	\$40	③ <input type="checkbox"/> 2-3		
Mexico City, Mexico	14	\$65	Kentuckiana (Louisville, KY)	37	\$30	North Texas (Dallas)	12	\$30	④ <input type="checkbox"/> 4-5		
Monterrey, Mexico	80	\$0	Detroit, MI	08	\$35	San Antonio/So. Texas	81	\$25	⑤ <input type="checkbox"/> More than 5		
Panama	94	\$20	Western Michigan (Grand Rapids)	38	\$25	<b>Western United States</b>			<b>Conferences attended annually (check one)</b>		
Lima, Peru	146	\$0	Minnesota (Minneapolis)	07	\$30	Phoenix, AZ	53	\$30	① <input type="checkbox"/> None		
Puerto Rico	86	\$30	Omaha, NE	23	\$30	Los Angeles, CA	01	\$25	② <input type="checkbox"/> 1		
Montevideo, Uruguay	133	*	Central Ohio (Columbus)	27	\$25	Orange County, CA (Anaheim)	79	\$30	③ <input type="checkbox"/> 2-3		
Venezuela	113	*	Greater Cincinnati, OH	03	\$20	Sacramento, CA	76	\$20	④ <input type="checkbox"/> 4-5		
<b>EUROPE/AFRICA</b>			Northeast Ohio (Cleveland)	26	\$30	San Francisco, CA	15	\$45	⑤ <input type="checkbox"/> More than 5		
Austria	157	\$50	Kettle Moraine, WI (Milwaukee)	57	\$25	San Diego, CA	19	\$30	<b>Primary reason for Joining the Association (check one)</b>		
Belux (Belgium and Luxembourg)	143	\$40	<b>Northeastern United States</b>			Silicon Valley, CA (Sunnyvale)	62	\$25	① <input type="checkbox"/> Discounts on Association products and services		
Czech Republic	153	\$110	Greater Hartford, CT (Southern New England)	28	\$35	Hawaii (Honolulu)	71	\$30	② <input type="checkbox"/> Subscription to <i>IS Control Journal</i>		
Denmark	96	*	Central Maryland (Baltimore)	24	\$25	Boise, ID	42	\$30	③ <input type="checkbox"/> Professional Advancement/ Certification		
Estonian	162	\$10	New England (Boston, MA)	18	\$30	<b>*Call Chapter for information</b>			④ <input type="checkbox"/> Access to Research, Publications, and Education		
Finland	115	\$70	New Jersey (Newark)	30	\$40				⑤ <input type="checkbox"/> Other_____		
Paris, France	75	*	Central New York (Syracuse)	29	\$30						
German	104	\$80	Hudson Valley, NY (Albany)	120	\$0						
Athens, Greece	134	\$10									
Budapest, Hungary	125	\$50									
Irish	156	\$35									
Tel-Aviv, Israel	40	*									
Milano, Italy	43	\$72									
Kenya	158	\$40									
Latvia	139	\$10									

## What does the Certified Information Systems Auditor credential mean to you?

### As an Employer

By hiring or retaining the services of a CISA, an organization has invested in a professional who has:

- Distinguished himself/herself from other industry professionals
- Followed a learning path to demonstrate IT assurance knowledge and skill
- Committed to maintaining skills through future professional development

For more than twenty years organizations have turned to professionals who have earned a CISA designation. CISAs have the proven ability to perform reviews in accordance with generally accepted standards and guidelines to ensure that the organization's information technology and business systems are adequately controlled, monitored and assessed.

### As an IT Professional

Earning the CISA designation helps assure a positive reputation as a qualified IS audit, control and/or security professional, and because the CISA program certifies individuals who demonstrate proficiency in today's most sought-after skills, employers prefer to hire and retain those who achieve and maintain their designation.

Although certification may not be mandatory for you at this time, a growing number of organizations are recommending employees to become certified. To help ensure your success in the global marketplace, it is vital that you select a certification program based on universally accepted technical practices. CISA delivers such a program. CISA is recognized worldwide, by all industries, as the preferred designation for IS audit, control and security professionals.

## Requirements for CISA certification

*See [www.isaca.org/cert1.htm](http://www.isaca.org/cert1.htm) for specific details.*

1. Successful completion of the CISA exam. The exam is offered annually at nearly 200 sites around the world in ten languages during the month of June.
2. Satisfy the work experience requirement pertaining to professional information systems (IS) auditing, control or security activity. Education waivers are available. See the CISA Bulletin of Information for details ([www.isaca.org/exam1.htm](http://www.isaca.org/exam1.htm)).
3. Adhere to the Information Systems Audit and Control Association's *Code of Professional Ethics* ([www.isaca.org/standard/code2.htm](http://www.isaca.org/standard/code2.htm))
4. Comply with annual continuing education requirements ([www.isaca.org/cisacep1.htm](http://www.isaca.org/cisacep1.htm))

Although COBIT is not specifically tested on the CISA examination, the COBIT control objectives or processes do reflect the tasks identified in the CISA Practice Analysis. As such, a thorough review of COBIT is recommended for candidate preparation for the CISA examination.

**For further information, please contact the Certification Department at [certification@isaca.org](mailto:certification@isaca.org) or by phone at +1.847.253.1545 ext. 474 or 471.**

# **COBIT®**

## **3rd Edition**

# **Executive Summary**

**July 2000**

Released by the COBIT Steering Committee and the IT Governance Institute™

### **The COBIT Mission:**

To research, develop, publicise and promote an authoritative, up-to-date, international set of generally accepted information technology control objectives for day-to-day use by business managers and auditors.

### Disclaimer

The Information Systems Audit and Control Foundation, IT Governance Institute and the sponsors of *COBIT: Control Objectives for Information and related Technology* have designed and created the publications entitled *Executive Summary*, *Framework*, *Control Objectives*, *Management Guidelines*, *Audit Guidelines* and *Implementation Tool Set* (collectively, the “Works”) primarily as an educational resource for controls professionals. The Information Systems Audit and Control Foundation, IT Governance Institute and the sponsors make no claim that use of any of the Works will assure a successful outcome. The Works should not be considered inclusive of any proper procedures and tests or exclusive of other procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific procedure or test, the controls professional should apply his or her own professional judgment to the specific control circumstances presented by the particular systems or IT environment.

### Disclosure and Copyright Notice

Copyright © 1996, 1998, 2000 by the Information Systems Audit and Control Foundation (ISACF). Reproduction for commercial purpose is not permitted without ISACF’s prior written permission. Permission is hereby granted to use and copy the *Executive Summary*, *Framework*, *Control Objectives*, *Management Guidelines* and *Implementation Tool Set* for non-commercial, internal use, including storage in a retrieval system and transmission by any means including, electronic, mechanical, recording or otherwise. All copies of the *Executive Summary*, *Framework*, *Control Objectives*, *Management Guidelines* and *Implementation Tool Set* must include the following copyright notice and acknowledgment: “Copyright 1996, 1998, 2000 Information Systems Audit and Control Foundation. Reprinted with the permission of the Information Systems Audit and Control Foundation and IT Governance Institute.”

The *Audit Guidelines* may not be used, copied, reproduced, modified, distributed, displayed, stored in a retrieval system, or transmitted in any form by any means (electronic, mechanical, photocopying, recording or otherwise), except with ISACF’s prior written authorization; provided, however, that the *Audit Guidelines* may be used for internal non-commercial purposes only. Except as stated herein, no other right or permission is granted with respect to this work. All rights in this work are reserved.

Information Systems Audit and Control Foundation  
IT Governance Institute  
3701 Algonquin Road, Suite 1010  
Rolling Meadows, IL 60008 USA  
Phone: +1.847.253.1545  
Fax: +1.847.253.1443  
E-mail: [research@isaca.org](mailto:research@isaca.org)  
Web sites: [www.ITgovernance.org](http://www.ITgovernance.org)  
[www.isaca.org](http://www.isaca.org)

ISBN 1-893209-15-6 (*Executive Summary*)  
ISBN 1-893209-13-X (Complete 6 book set with CD-ROM)

Printed in the United States of America.



## EXECUTIVE OVERVIEW

**C**ritically important to the survival and success of an organisation is effective management of information and related Information Technology (IT). In this global information society—where information travels through cyberspace without the constraints of time, distance and speed—this criticality arises from the:

- Increasing dependence on information and the systems that deliver this information
- Increasing vulnerabilities and a wide spectrum of threats, such as cyber threats and information warfare
- Scale and cost of the current and future investments in information and information systems
- Potential for technologies to dramatically change organisations and business practices, create new opportunities and reduce costs

For many organisations, information and the technology that supports it represent the organisation's most valuable assets. Moreover, in today's very competitive and rapidly changing business environment, management has heightened expectations regarding IT delivery functions: management requires increased quality, functionality and ease of use; decreased delivery time; and continuously improving service levels—while demanding that this be accomplished at lower costs.

***Many organisations recognise the potential benefits that technology can yield. Successful organisations, however, understand and manage the risks associated with implementing new technologies.***

There are numerous changes in IT and its operating environment that emphasise the need to better manage IT-related risks. Dependence on electronic information and IT systems is essential to support critical business processes. In addition, the regulatory environment is mandating stricter control over information. This, in turn, is driven by increasing disclosures of information system disasters and increasing electronic fraud. The management of IT-related risks is now being understood as a key part of enterprise governance.

Within enterprise governance, IT governance is becoming more and more prominent, and is defined as a structure of relationships and processes to direct and control the enterprise in order to achieve the enterprise's goals by adding value while balancing risk versus return over IT and its processes. IT governance is integral to the success of enterprise governance by assuring efficient and effective measurable improvements in related enterprise processes. IT governance provides the structure that links IT processes, IT resources and information to enterprise strategies and objectives. Furthermore, IT governance integrates and institutionalises good (or best) practices of planning and organising,

acquiring and implementing, delivering and supporting, and monitoring IT performance to ensure that the enterprise's information and related technology support its business objectives. IT governance thus enables the enterprise to take full advantage of its information, thereby maximising benefits, capitalising on opportunities and gaining competitive advantage.

### IT GOVERNANCE

**A structure of relationships and processes to direct and control the enterprise in order to achieve the enterprise's goals by adding value while balancing risk versus return over IT and its processes.**

**O**rganisations must satisfy the quality, fiduciary and security requirements for their information, as for all assets. Management must also optimise the use of available resources, including data, application systems, technology, facilities and people. To discharge these responsibilities, as well as to achieve its objectives, management must understand the status of its own IT systems and decide what security and control they should provide.

Control Objectives for Information and related Technology (COBIT), now in its 3<sup>rd</sup> edition, helps meet the multiple needs of management by bridging the gaps between business risks, control needs and technical issues. It provides good practices across a domain and process framework and presents activities in a manageable and logical structure. COBIT's "good practices" means consensus of the experts—they will help optimise information investments and will provide a measure to be judged against when things do go wrong.

Management must ensure that an internal control system or framework is in place which supports the business processes, makes it clear how each individual control activity satisfies the information requirements and impacts the IT resources. Impact on IT resources is highlighted in the COBIT *Framework* together with the business requirements for effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability of information that need to be satisfied. Control, which includes policies, organisational structures, practices and procedures, is management's responsibility. Management, through its enterprise governance, must ensure that due diligence is exercised by all individuals involved in the management, use, design, development, maintenance or operation of information systems. An IT control objective is a statement of the desired result or purpose to be achieved by implementing control procedures within a particular IT activity.

**B**usiness orientation is the main theme of COBIT. It is designed to be employed not only by users and auditors, but also, and more importantly, as comprehensive guidance for management and business process owners. Increasingly, business practice involves the full empowerment of business process owners so they have total responsibility for all aspects of the business process. In particular, this includes providing adequate controls.

The COBIT *Framework* provides a tool for the business process owner that facilitates the discharge of this responsibility. The *Framework* starts from a simple and pragmatic premise:

*In order to provide the information that the organisation needs to achieve its objectives, IT resources need to be managed by a set of naturally grouped processes.*

The *Framework* continues with a set of 34 high-level *Control Objectives*, one for each of the IT processes, grouped into four domains: planning and organisation, acquisition and implementation, delivery and support, and monitoring. This structure covers all aspects of information and the technology that supports it. By addressing these 34 high-level control objectives, the business process owner can ensure that an adequate control system is provided for the IT environment.

**I**T governance guidance is also provided in the COBIT *Framework*. IT governance provides the structure that links IT processes, IT resources and information to enterprise strategies and objectives. IT governance integrates optimal ways of planning and organising, acquiring and implementing, delivering and supporting, and monitoring IT performance. IT governance enables the enterprise to take full advantage of its information, thereby maximising benefits, capitalising on opportunities and gaining competitive advantage.

In addition, corresponding to each of the 34 high-level control objectives is an *Audit Guideline* to enable the review of IT processes against COBIT's 318 recommended detailed control objectives to provide management assurance and/or advice for improvement.

**T**he *Management Guidelines*, COBIT's most recent development, further enhances and enables enterprise management to deal more effectively with the needs and requirements of IT governance. The guidelines are action oriented and generic and provide management direction for getting the enterprise's information and related processes under control, for monitoring achievement of organisational goals, for monitoring performance within each IT process and for benchmarking organisational achievement.

Specifically, COBIT provides **Maturity Models** for control over IT processes, so that management can map where the organisation is today, where it stands in relation to the best-in-class in its industry and to international standards and where the organisation wants to be; **Critical Success Factors**, which define the most important management-oriented implementation guidelines to achieve control over and within its IT processes; **Key Goal Indicators**, which define measures that tell management—after the fact—whether an IT process has achieved its business requirements; and **Key Performance Indicators**, which are lead indicators that define measures of how well the IT process is performing in enabling the goal to be reached.

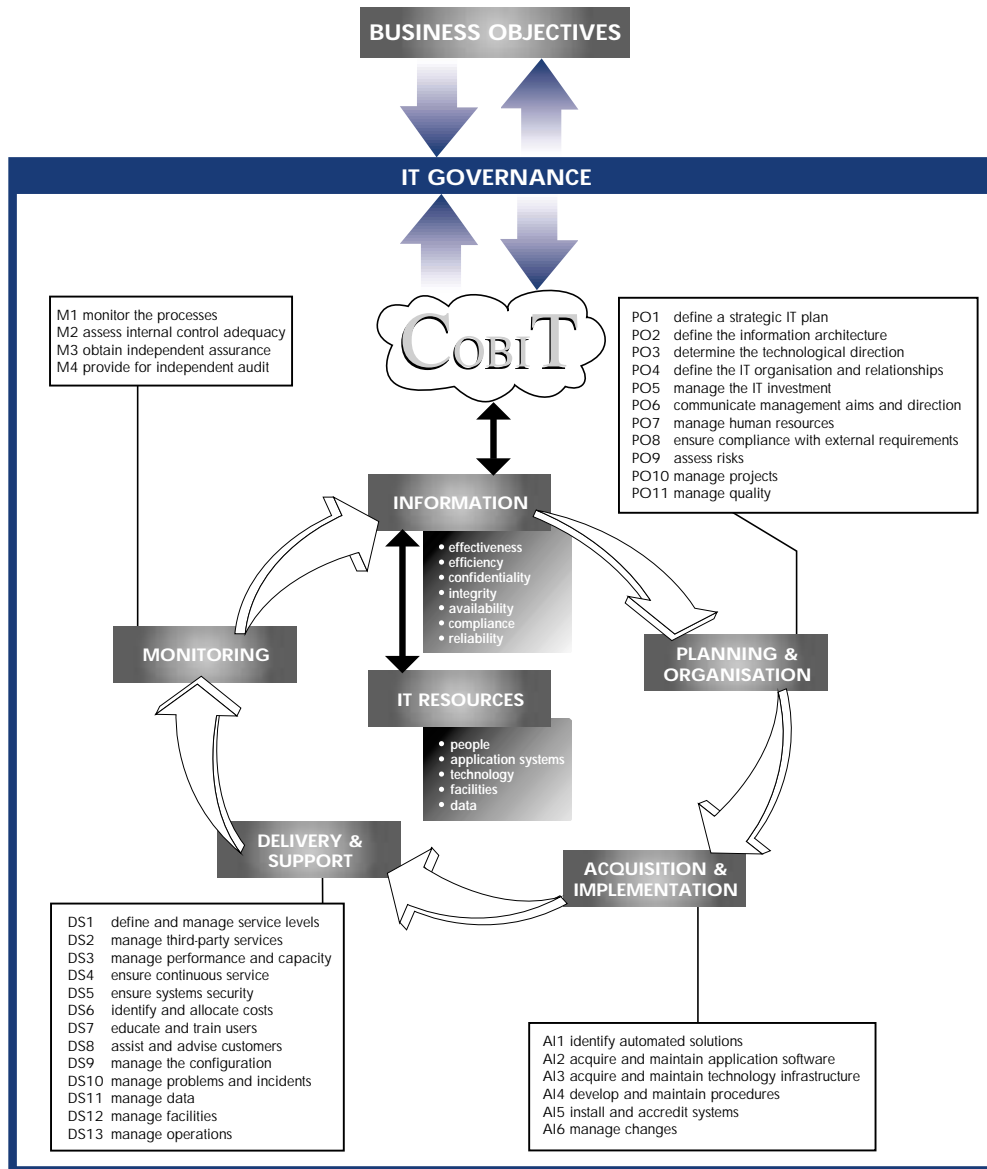
COBIT's *Management Guidelines* are generic and action oriented for the purpose of answering the following types of management questions: How far should we go, and is the cost justified by the benefit? What are the indicators of good performance? What are the critical success factors? What are the risks of not achieving our objectives? What do others do? How do we measure and compare?

COBIT also contains an *Implementation Tool Set* that provides lessons learned from those organisations that quickly and successfully applied COBIT in their work environments. It has two particularly useful tools—Management Awareness Diagnostic and IT Control Diagnostic—to assist in analysing an organisation's IT control environment.

Over the next few years, the management of organisations will need to demonstrably attain increased levels of security and control. COBIT is a tool that allows managers to bridge the gap with respect to control requirements, technical issues and business risks and communicate that level of control to stakeholders. COBIT enables the development of clear policy and good practice for IT control throughout organisations, worldwide. **Thus, COBIT is designed to be the breakthrough IT governance tool that helps in understanding and managing the risks and benefits associated with information and related IT.**

# EXECUTIVE SUMMARY

## COBIT IT PROCESSES DEFINED WITHIN THE FOUR DOMAINS



## THE COBIT FRAMEWORK

### THE NEED FOR CONTROL IN INFORMATION TECHNOLOGY

In recent years, it has become increasingly evident that there is a need for a reference framework for security and control in IT. Successful organisations require an appreciation for and a basic understanding of the risks and constraints of IT at all levels within the enterprise in order to achieve effective direction and adequate controls.

**MANAGEMENT** has to decide what to reasonably invest for security and control in IT and how to balance risk and control investment in an often unpredictable IT environment. While information systems security and control help manage risks, they do not eliminate them. In addition, the exact level of risk can never be known since there is always some degree of uncertainty. Ultimately, management must decide on the level of risk it is willing to accept. Judging what level can be tolerated, particularly when weighted against the cost, can be a difficult management decision. Therefore, management clearly needs a framework of generally accepted IT security and control practices to benchmark the existing and planned IT environment.

There is an increasing need for **USERS** of IT services to be assured, through accreditation and audit of IT services provided by internal or third parties, that adequate security and control exists. At present, however, the implementation of good IT controls in information systems, be they commercial, non-profit or governmental, is hampered by confusion. The confusion arises from the different evaluation methods such as ITSEC, TCSEC, ISO 9000 evaluations, emerging COSO internal control evaluations, etc. As a result, users need a general foundation to be established as a first step.

Frequently, **AUDITORS** have taken the lead in such international standardisation efforts because they are continuously confronted with the need to substantiate their opinion on internal control to management. Without a framework, this is an exceedingly difficult task. Furthermore, auditors are increasingly being called on by management to proactively consult and advise on IT security and control-related matters.

### THE BUSINESS ENVIRONMENT: COMPETITION, CHANGE AND COST

Global competition is here. Organisations are restructuring to streamline operations and simultaneously take advantage of the advances in IT to improve their competitive position. Business re-engineering, right-sizing, outsourcing, empowerment, flattened organisations and distributed processing are all changes that impact the way that business and governmental organisations operate. These changes are having, and will continue to have, profound implications for the management and operational control structures within organisations worldwide.

Emphasis on attaining competitive advantage and cost-efficiency implies an ever-increasing reliance on technology as a major component in the strategy of most organisations. Automating organisational functions is, by its very nature, dictating the incorporation of more powerful control mechanisms into computers and networks, both hardware-based and software-based. Furthermore, the fundamental structural characteristics of these controls are evolving at the same rate and in the same “leap frog” manner as the underlying computing and networking technologies are evolving.

Within the framework of accelerated change, if managers, information systems specialists and auditors are indeed going to be able to effectively fulfil their roles, their skills must evolve as rapidly as the technology and the environment. One must understand the technology of controls involved and its changing nature if one is to exercise reasonable and prudent judgments in evaluating control practices found in typical business or governmental organisations.

### EMERGENCE OF ENTERPRISE AND IT GOVERNANCE

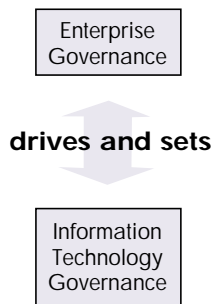
To achieve success in this information economy, enterprise governance and IT governance can no longer be considered separate and distinct disciplines. Effective enterprise governance focuses individual and group expertise and experience where it can be most productive, monitors and measures performance and provides assurance to critical issues. IT, long considered solely an

# EXECUTIVE SUMMARY

enabler of an enterprise's strategy, must now be regarded as an integral part of that strategy.

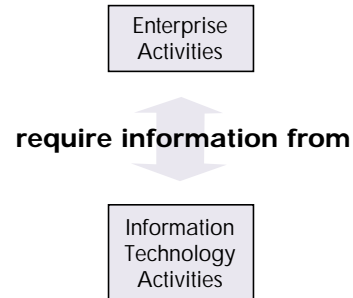
IT governance provides the structure that links IT processes, IT resources, and information to enterprise strategies and objectives. IT governance integrates and institutionalises optimal ways of planning and organising, acquiring and implementing, delivering and supporting, and monitoring IT performance. IT governance is integral to the success of enterprise governance by assuring efficient and effective measurable improvements in related enterprise processes. IT governance enables the enterprise to take full advantage of its information, thereby maximising benefits, capitalising on opportunities and gaining competitive advantage.

Looking at the interplay of enterprise and IT governance processes in more detail, enterprise governance, the system by which entities are directed and controlled, drives and sets IT governance. At the same time, IT should provide critical input to, and constitute an important component of, strategic plans. IT may in fact influence strategic opportunities outlined by the enterprise.

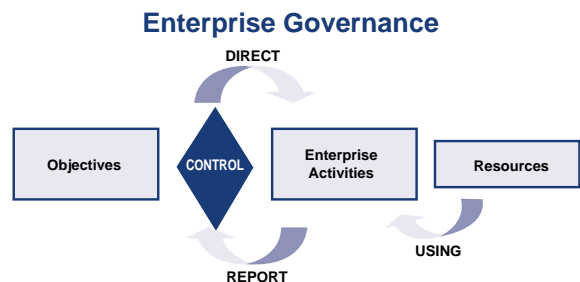


Enterprise activities require information from IT activities in order to meet business objectives. Successful organisations ensure interdependence between their

strategic planning and their IT activities. IT must be aligned with and enable the enterprise to take full advantage of its information, thereby maximising benefits, capitalising on opportunities and gaining a competitive advantage.



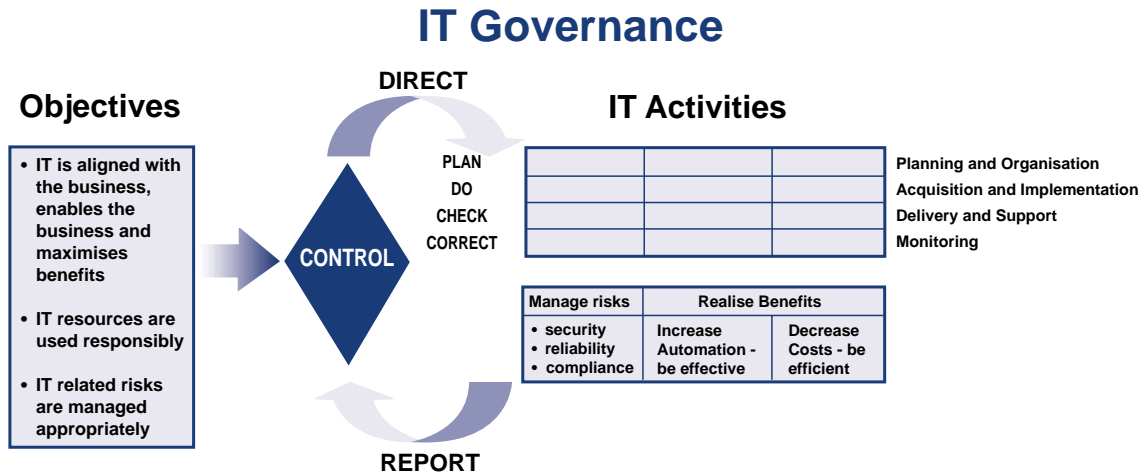
Enterprises are governed by generally accepted good (or best) practices, to ensure that the enterprise is achieving its goals—the assurance of which is guaranteed by certain controls. From these objectives flows the organisation's direction, which dictates certain enterprise activities, using the enterprise's resources. The results of the enterprise activities are measured and reported on, providing input to the constant revision and maintenance of the controls, beginning the cycle again.



## THE COBIT FRAMEWORK, *continued*

IT also is governed by good (or best) practices, to ensure that the enterprise's information and related technology support its business objectives, its resources are used responsibly and its risks are managed appropriately. These practices form a basis for direction of IT activities, which can be characterised as planning and organising, acquiring and implementing, delivering and sup-

porting, and monitoring, for the dual purposes of managing risks (to gain security, reliability and compliance) and realising benefits (increasing effectiveness and efficiency). Reports are issued on the outcomes of IT activities, which are measured against the various practices and controls, and the cycle begins again.



In order to ensure that management reaches its business objectives, it must direct and manage IT activities to reach an effective balance between managing risks and realising benefits. To accomplish this, management needs to identify the most important activities to be performed, measure progress towards achieving goals and determine how well the IT processes are performing. In addition, it needs the ability to evaluate the organisation's maturity level against industry best practices and international standards. **To support these management needs, the COBIT Management Guidelines have identified specific Critical Success Factors, Key Goal Indicators, Key Performance Indicators and an associated Maturity Model for IT governance, as presented in Appendix I.**

### RESPONSE TO THE NEED

In view of these ongoing changes, the development of this framework for control objectives for IT, along with continued applied research in IT controls based on this framework, are cornerstones for effective progress in the field of information and related technology controls.

On the one hand, we have witnessed the development and publication of overall business control models like COSO (Committee of Sponsoring Organisations of the Treadway Commission—*Internal Control-Integrated Framework*, 1992) in the US, Cadbury in the UK, CoCo in Canada and King in South Africa. On the other hand,

an important number of more focused control models are in existence at the level of IT. Good examples of the latter category are the Security Code of Conduct from DTI (Department of Trade and Industry, UK), Information Technology Control Guidelines from CICA (Canadian Institute of Chartered Accountants, Canada), and the Security Handbook from NIST (National Institute of Standards and Technology, US). However, these focused control models do not provide a comprehensive and usable control model over IT in support of business processes. The purpose of COBIT is to bridge this gap by providing a foundation that is closely linked to business objectives while focusing on IT.



# EXECUTIVE SUMMARY

(Most closely related to COBIT is the recently published *AICPA/CICA SysTrust™ Principles and Criteria for Systems Reliability*. SysTrust is an authoritative issuance of both the Assurance Services Executive Committee in the United States and the Assurance Services Development Board in Canada, based in part on the COBIT *Control Objectives*. SysTrust is designed to increase the comfort of management, customers and business partners with the systems that support a business or a particular activity. The SysTrust service entails the public accountant providing an assurance service in which he or she evaluates and tests whether a system is reliable when measured against four essential principles: availability, security, integrity and maintainability.)

A focus on the business requirements for controls in IT and the application of emerging control models and related international standards evolved the original Information Systems Audit and Control Foundation's *Control Objectives* from an auditor's tool to COBIT, a management tool. Further, the development of IT *Management Guidelines* has taken COBIT to the next level—providing management with Key Goal Indicators (KGIs), Key Performance Indicators (KPIs), Critical Success Factors (CSFs) and Maturity Models so that it can assess its IT environment and make choices for control implementation and control improvements over the organisation's information and related technology.

Hence, the main objective of the COBIT project is the development of clear policies and good practices for security and control in IT for worldwide endorsement by commercial, governmental and professional organisations. It is the goal of the project to develop these control objectives primarily from the business objectives and needs perspective. (This is compliant with the COSO perspective, which is first and foremost a management framework for internal controls.) Subsequently, control objectives have been developed from the audit objectives (certification of financial information, certification of internal control measures, efficiency and effectiveness, etc.) perspective.

## AUDIENCE: MANAGEMENT, USERS AND AUDITORS

COBIT is designed to be used by three distinct audiences.

### MANAGEMENT:

to help them balance risk and control investment in an often unpredictable IT environment.

### USERS:

to obtain assurance on the security and controls of IT services provided by internal or third parties.

### AUDITORS:

to substantiate their opinions and/or provide advice to management on internal controls.

## BUSINESS OBJECTIVES ORIENTATION

COBIT is aimed at addressing business objectives. The control objectives make a clear and distinct link to business objectives in order to support significant use outside the audit community. Control objectives are defined in a process-oriented manner following the principle of business re-engineering. At identified domains and processes, a high-level control objective is identified and rationale provided to document the link to the business objectives. In addition, considerations and guidelines are provided to define and implement the IT control objective.

The classification of domains where high-level control objectives apply (domains and processes), an indication of the business requirements for information in that domain, as well as the IT resources primarily impacted by the control objectives, together form the COBIT *Framework*. The *Framework* is based on the research activities that have identified 34 high-level control objectives and 318 detailed control objectives. The *Framework* was exposed to the IT industry and the audit profession to allow an opportunity for review, challenge and comment. The insights gained have been appropriately incorporated.

## THE COBIT FRAMEWORK, *continued*

### GENERAL DEFINITIONS

For the purpose of this project, the following definitions are provided. “Control” is adapted from the COSO Report (*Internal Control—Integrated Framework*, Committee of Sponsoring Organisations of the Treadway Commission, 1992) and “IT Control Objective” is adapted from the SAC Report (*Systems Auditability and Control Report*, The Institute of Internal Auditors Research Foundation, 1991 and 1994).

#### Control is defined as

the policies, procedures, practices and organisational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected.

#### IT Control Objective is defined as

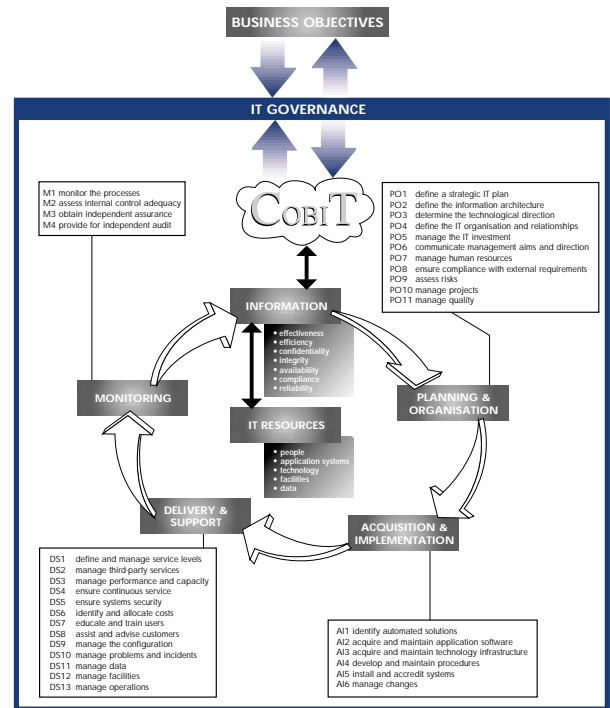
a statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity.

#### IT Governance is defined as

a structure of relationships and processes to direct and control the enterprise in order to achieve the enterprise’s goals by adding value while balancing risk versus return over IT and its processes.

The diagram below illustrates COBIT’s basic concept: in order to provide the information that the organisation needs to achieve its objectives, IT governance must be exercised by the organisation to ensure that IT resources are managed by a set of naturally grouped IT processes.

### COBIT IT PROCESSES DEFINED WITHIN THE FOUR DOMAINS





# EXECUTIVE SUMMARY

## COBIT HISTORY AND BACKGROUND

COBIT 3<sup>rd</sup> Edition is the most recent version of Control Objectives for Information and related Technology, first released by the Information Systems Audit and Control Foundation (ISACF) in 1996. The 2<sup>nd</sup> edition, reflecting an increase in the number of source documents, a revision in the high-level and detailed control objectives and the addition of the *Implementation Tool Set*, was published in 1998. The 3<sup>rd</sup> edition marks the entry of a new primary publisher for COBIT: the IT Governance Institute.

The IT Governance Institute was formed by the Information Systems Audit and Control Association (ISACA) and its related Foundation in 1998 in order to advance the understanding and adoption of IT governance principles. Due to the addition of the *Management Guidelines* to COBIT 3<sup>rd</sup> Edition and its expanded and enhanced focus on IT governance, the IT Governance Institute took a leading role in the publication's development.

COBIT was originally based on ISACF's *Control Objectives*, and has been enhanced with existing and emerging international technical, professional, regulatory and industry-specific standards. The resulting control objectives have been developed for application to organisation-wide information systems. The term "generally applicable and accepted" is explicitly used in the same sense as Generally Accepted Accounting Principles (GAAP).

COBIT is relatively small in size and attempts to be both pragmatic and responsive to business needs while being independent of the technical IT platforms adopted in an organisation.

While not excluding any other accepted standard in the information systems control field that may have come to light during the research, sources identified are:

**Technical standards** from ISO, EDIFACT, etc.

**Codes of Conduct** issued by the Council of Europe, OECD, ISACA, etc.

**Qualification criteria** for IT systems and processes: ITSEC, TCSEC, ISO 9000, SPICE, TickIT, Common Criteria, etc.

**Professional standards** for internal control and auditing: COSO, IFAC, AICPA, CICA, ISACA, IIA, PCIE, GAO, etc.

**Industry practices and requirements** from industry forums (ESF, I4) and government-sponsored platforms (IBAG, NIST, DTI), etc., and

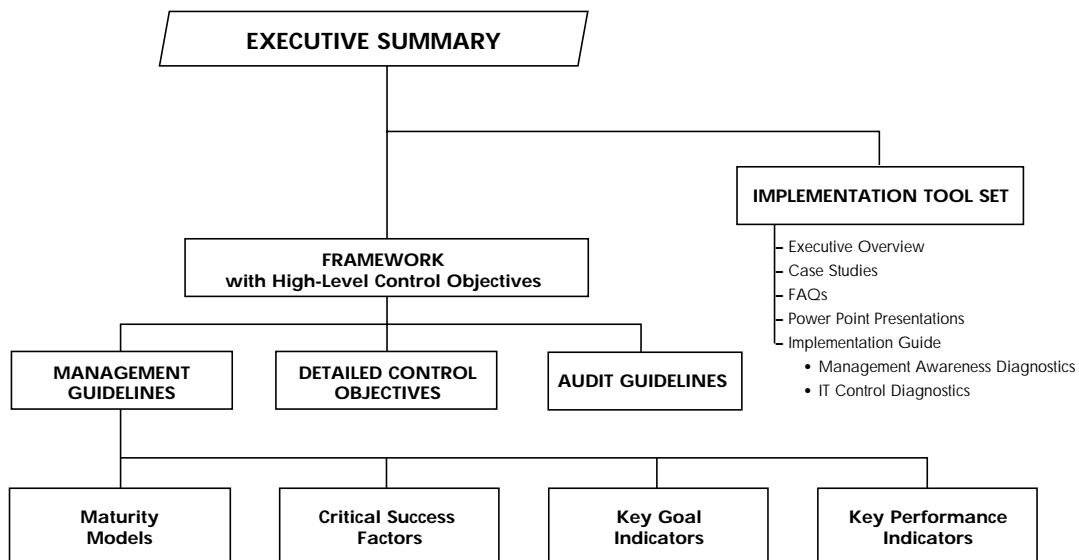
**Emerging industry-specific requirements** from banking, electronic commerce, and IT manufacturing.

## COBIT PRODUCT EVOLUTION

COBIT will evolve over the years and be the foundation for further research. Thus, a family of COBIT products will be created and, as this occurs, the IT tasks and activities that serve as the structure to organise control objectives will be further refined, and the balance between domains and processes reviewed in light of the industry's changing landscape.

Research and publication have been made possible by significant grants from PricewaterhouseCoopers and donations from ISACA chapters and members worldwide. The European Security Forum (ESF) kindly made research material available to the project. The Gartner Group also participated in the development and provided quality assurance review of the *Management Guidelines*.

## COBIT Family of Products



### IT GOVERNANCE MANAGEMENT GUIDELINE

The following Management Guideline and Maturity Model identify the Critical Success Factors (CSFs), Key Goal Indicators (KGIs), Key Performance Indicators (KPIs) and Maturity Model for **IT governance**. First, IT governance is defined, articulating the business need. Next, the information criteria related to IT governance are identified. The business need is measured by the KGIs and enabled by a control statement, leveraged by all the IT resources. The achievement of the enabling control statement is measured by the KPIs, which consider the CSFs. The Maturity Model is used to evaluate an organisation's level of achievement of IT governance—from Non-existent (the lowest level) to Initial/Ad Hoc, to Repeatable but Intuitive, to Defined Process, to Managed and Measurable, to Optimised (the highest level). To achieve the Optimised maturity level for IT governance, an organisation must be at least at the Optimised level for the Monitoring domain and at least at the Managed and Measurable level for all other domains.

(See the COBIT *Management Guidelines* for a thorough discussion of the use of these tools.)

## IT GOVERNANCE MANAGEMENT GUIDELINE

Governance over information technology and its processes with the business goal of adding value, while balancing risk versus return

ensures delivery of information to the business that addresses the required **Information Criteria** and is measured by **Key Goal Indicators**

is enabled by *creating and maintaining a system of process and control excellence appropriate for the business that directs and monitors the business value delivery of IT*

considers **Critical Success Factors** that leverage all **IT Resources** and is measured by **Key Performance Indicators**

### Information Criteria

effectiveness
efficiency
confidentiality
integrity
availability
compliance
reliability

### IT Resources

people
applications
technology
facilities
data

### Key Goal Indicators

- Enhanced performance and cost management
- Improved return on major IT investments
- Improved time to market
- Increased quality, innovation and risk management
- Appropriately integrated and standardised business processes
- Reaching new and satisfying existing customers
- Availability of appropriate bandwidth, computing power and IT delivery mechanisms
- Meeting requirements and expectations of the customer of the process on budget and on time
- Adherence to laws, regulations, industry standards and contractual commitments
- Transparency on risk taking and adherence to the agreed organisational risk profile
- Benchmarking comparisons of IT governance maturity
- Creation of new service delivery channels

### Key Performance Indicators

- Improved cost-efficiency of IT processes (costs vs. deliverables)
- Increased number of IT action plans for process improvement initiatives
- Increased utilisation of IT infrastructure
- Increased satisfaction of stakeholders (survey and number of complaints)
- Improved staff productivity (number of deliverables) and morale (survey)
- Increased availability of knowledge and information for managing the enterprise
- Increased linkage between IT and enterprise governance
- Improved performance as measured by IT balanced scorecards

### Critical Success Factors

- IT governance activities are integrated into the enterprise governance process and leadership behaviours
- IT governance focuses on the enterprise goals, strategic initiatives, the use of technology to enhance the business and on the availability of sufficient resources and capabilities to keep up with the business demands
- IT governance activities are defined with a clear purpose, documented and implemented, based on enterprise needs and with unambiguous accountabilities
- Management practices are implemented to increase efficient and optimal use of resources and increase the effectiveness of IT processes
- Organisational practices are established to enable: sound oversight; a control environment/culture; risk assessment as standard practice; degree of adherence to established standards; monitoring and follow up of control deficiencies and risks
- Control practices are defined to avoid breakdowns in internal control and oversight
- There is integration and smooth interoperability of the more complex IT processes such as problem, change and configuration management
- An audit committee is established to appoint and oversee an independent auditor, focusing on IT when driving audit plans, and review the results of audits and third-party reviews.

## IT Governance Maturity Model

Governance over information technology and its processes with the business goal of adding value, while balancing risk versus return

- 0 Non-existent** There is a complete lack of any recognisable IT governance process. The organisation has not even recognised that there is an issue to be addressed and hence there is no communication about the issue.
- 1 Initial /Ad Hoc** There is evidence that the organisation has recognised that IT governance issues exist and need to be addressed. There are, however, no standardised processes, but instead there are ad hoc approaches applied on an individual or case-by-case basis. Management's approach is chaotic and there is only sporadic, non-consistent communication on issues and approaches to address them. There may be some acknowledgement of capturing the value of IT in outcome-oriented performance of related enterprise processes. There is no standard assessment process. IT monitoring is only implemented reactively to an incident that has caused some loss or embarrassment to the organisation.
- 2 Repeatable but Intuitive** There is global awareness of IT governance issues. IT governance activities and performance indicators are under development, which include IT planning, delivery and monitoring processes. As part of this effort, IT governance activities are formally established into the organisation's change management process, with active senior management involvement and oversight. Selected IT processes are identified for improving and/or controlling core enterprise processes and are effectively planned and monitored as investments, and are derived within the context of a defined IT architectural framework. Management has identified basic IT governance measurements and assessment methods and techniques, however, the process has not been adopted across the organisation. There is no formal training and communication on governance standards and responsibilities are left to the individual. Individuals drive the governance processes within various IT projects and processes. Limited governance tools are chosen and implemented for gathering governance metrics, but may not be used to their full capacity due to a lack of expertise in their functionality.
- 3 Defined Process** The need to act with respect to IT governance is understood and accepted. A baseline set of IT governance indicators is developed, where linkages between outcome measures and performance drivers are defined, documented and integrated into strategic and operational planning and monitoring processes. Procedures have been standardised, documented and implemented. Management has communicated standardised procedures and informal training is established. Performance indicators over all IT governance activities are being recorded and tracked, leading to enterprise-wide improvements. Although measurable, procedures are not sophisticated, but are the formalisation of existing practices. Tools are standardised, using currently available techniques. IT Balanced Business Scorecard ideas are being adopted by the organization. It is, however, left to the individual to get training, to follow the standards and to apply them. Root cause analysis is only occasionally applied. Most processes are monitored against some (baseline) metrics, but any deviation, while mostly being acted upon by individual initiative, would unlikely be detected by management. Nevertheless, overall accountability of key process performance is clear and management is rewarded based on key performance measures.
- 4 Managed and Measurable** There is full understanding of IT governance issues at all levels, supported by formal training. There is a clear understanding of who the customer is and responsibilities are defined and monitored through service level agreements. Responsibilities are clear and process ownership is established. IT processes are aligned with the business and with the IT strategy. Improvement in IT processes is based primarily upon a quantitative understanding and it is possible to monitor and measure compliance with procedures and process metrics. All process stakeholders are aware of risks, the importance of IT and the opportunities it can offer. Management has defined tolerances under which processes must operate. Action is taken in many, but not all cases where processes appear not to be working effectively or

efficiently. Processes are occasionally improved and best internal practices are enforced. Root cause analysis is being standardised. Continuous improvement is beginning to be addressed. There is limited, primarily tactical, use of technology, based on mature techniques and enforced standard tools. There is involvement of all required internal domain experts. IT governance evolves into an enterprise-wide process. IT governance activities are becoming integrated with the enterprise governance process.

- 5 **Optimised** There is advanced and forward-looking understanding of IT governance issues and solutions. Training and communication is supported by leading-edge concepts and techniques. Processes have been refined to a level of external best practice, based on results of continuous improvement and maturity modeling with other organisations. The implementation of these policies has led to an organisation, people and processes that are quick to adapt and fully support IT

governance requirements. All problems and deviations are root cause analysed and efficient action is expediently identified and initiated. IT is used in an extensive, integrated and optimised manner to automate the workflow and provide tools to improve quality and effectiveness. The risks and returns of the IT processes are defined, balanced and communicated across the enterprise. External experts are leveraged and benchmarks are used for guidance. Monitoring, self-assessment and communication about governance expectations are pervasive within the organisation and there is optimal use of technology to support measurement, analysis, communication and training. Enterprise governance and IT governance are strategically linked, leveraging technology and human and financial resources to increase the competitive advantage of the enterprise.

AMERICAN SAMOA  
ARGENTINA  
ARMENIA  
AUSTRALIA  
AUSTRIA  
BAHAMAS  
BAHRAIN  
BANGLADESH  
BARBADOS  
BELGIUM  
BERMUDA  
BOLIVIA  
BOTSWANA  
BRAZIL  
BRITISH VIRGIN ISLANDS  
CANADA  
CAYMAN ISLANDS  
CHILE  
CHINA  
COLOMBIA  
COSTA RICA  
CROATIA  
CURACAO  
CYPRUS  
CZECH REPUBLIC  
DENMARK  
DOMINICAN REPUBLIC  
ECUADOR  
EGYPT  
EL SALVADOR  
ESTONIA  
FAEROE ISLANDS  
FIJI  
FINLAND  
FRANCE  
GERMANY  
GHANA  
GREECE  
GUAM  
GUATEMALA  
HONDURAS  
HONG KONG  
HUNGARY  
ICELAND  
INDIA  
INDONESIA  
IRAN  
IRELAND  
ISRAEL  
ITALY  
IVORY COAST  
JAMAICA  
JAPAN  
JORDAN  
KAZAKHSTAN  
KENYA  
KOREA  
KUWAIT

# INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION

## A Single International Source for Information Technology Controls

*The Information Systems Audit and Control Association is a leading global professional organisation representing individuals in more than 100 countries and comprising all levels of IT — executive, management, middle management and practitioner. The Association is uniquely positioned to fulfil the role of a central, harmonising source of IT control practice standards for the world over. Its strategic alliances with other groups in the financial, accounting, auditing and IT professions are ensuring an unparalleled level of integration and commitment by business process owners.*

### Association Programmes and Services

*The Association's services and programmes have earned distinction by establishing the highest levels of excellence in certification, standards, professional education and technical publishing.*

- *Its certification programme (the Certified Information Systems Auditor™) is the only global designation throughout the IT audit and control community.*
- *Its standards activities establish the quality baseline by which other IT audit and control activities are measured.*

- *Its professional education programme offers technical and management conferences on five continents, as well as seminars worldwide to help professionals everywhere receive high-quality continuing education.*
- *Its technical publishing area provides references and professional development materials to augment its distinguished selection of programmes and services.*

*The Information Systems Audit and Control Association was formed in 1969 to meet the unique, diverse and high technology needs of the burgeoning IT field. In an industry in which progress is measured in nano-seconds, ISACA has moved with agility and speed to bridge the needs of the international business community and the IT controls profession.*

### For More Information

*To receive additional information, you may telephone (+1.847.253.1545), send an e-mail ([research@isaca.org](mailto:research@isaca.org)) or visit these web sites:*

**[www.ITgovernance.org](http://www.ITgovernance.org)**  
**[www.isaca.org](http://www.isaca.org)**

LATVIA  
LEBANON  
LIECHTENSTEIN  
LITHUANIA  
LUXEMBURG  
MALAYSIA  
MALTA  
MALAWI  
MAURITIUS  
MEXICO  
NAMIBIA  
NEPAL  
NETHERLANDS  
NEW GUINEA  
NEW ZEALAND  
NICARAGUA  
NIGERIA  
NORWAY  
OMAN  
PAKISTAN  
PANAMA  
PARAGUAY  
PERU  
PHILIPPINES  
POLAND  
PORTUGAL  
QATAR  
RUSSIA  
SAUDI ARABIA  
SCOTLAND  
SEYCHELLES  
SINGAPORE  
SLOVAK REPUBLIC  
SLOVENIA  
SOUTH AFRICA  
SPAIN  
SRI LANKA  
ST. KITTS  
ST. LUCIA  
SWEDEN  
SWITZERLAND  
TAIWAN  
TANZANIA  
TASMANIA  
THAILAND  
TRINIDAD & TOBAGO  
TUNISIA  
TURKEY  
UGANDA  
UNITED ARAB EMIRATES  
UNITED KINGDOM  
UNITED STATES  
URUGUAY  
VENEZUELA  
VIETNAM  
WALES  
YUGOSLAVIA  
ZAMBIA  
ZIMBABWE